AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A security analysis tool for an automation system having a controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the security analysis tool comprising:

~~an interface component that generates a description of one or more industrial controllers, wherein the description includes at least one of shop floor access patterns, Intranet access patterns, Internet access patterns, or wireless access patterns~~;

a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication; and

an analyzer component that monitors data traffic subsequent to the training period and generates one or more security outputs ~~based on the description~~ if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation, the one or more security outputs including at least one output ~~deployed to the one or more industrial controllers that adjusts a security parameter~~ that alters the data traffic between the controller and the at least one I/O device, ~~associated with the one or more industrial controllers; and~~

~~a validation component that periodically monitors the one or more industrial controllers following deployment of the one or more security outputs to determine one or more vulnerabilities related thereto~~.

2. (Currently Amended) The tool of claim 1, ~~at least one of the interface component or the analyzer component operate on a computer and receive one or more factory inputs that provide the description~~ further comprising an interface component that generates a description of one or more industrial controllers in the automation system.

3. (Currently Amended) The tool of claim 2, wherein at least one of the interface component or the analyzer component operate on a computer and receive one or more factory inputs that provide the description, the factory inputs include at least one of user input, model inputs, schemas, formulas, equations, files, maps, or codes.

4. (Currently Amended) The tool of claim [[2]] 3, wherein the factory inputs are processed by the analyzer component to generate the security outputs, the security outputs including at least one of manuals, documents, schemas, executables, codes, files, e-mails, recommendations, topologies, configurations, application procedures, parameters, policies, rules, user procedures, or user practices that are employed to facilitate security measures in an automation system.

5. (Currently Amended) The tool of claim [[1]] 2, wherein the interface component includes at least one of a display output having associated display objects and at least one input to facilitate operations with the analyzer component, the interface component is associated with at least one of an engine, an application, an editor tool, a web browser, or a web service.

6. (Currently Amended) The tool of claim 5, wherein the display objects include at least one of configurable icons, buttons, sliders, input boxes, selection options, menus, or tabs, the display objects having multiple configurable dimensions, shapes, colors, text, data and sounds to facilitate operations with the analyzer component.

7. (Currently Amended) The tool of claim 5, the at least one input includes ~~receiving~~ user commands from at least one of a mouse, a keyboard, speech input, a web site, a remote web service, a camera, or video input to affect operations of the interface component and the analyzer component.

8. (Currently Amended) The tool of claim [[1]] 2, wherein the description includes a model of one or more industrial automation assets to be protected and associated network pathways to access the one or more industrial automation assets.

9. (Currently Amended) The tool of claim [[1]] 2, wherein the description includes at least one of risk data or cost data that is employed by the analyzer component to determine suitable security measures.

10-11. (Cancelled)

12. (Currently Amended) A security analysis method for use in an industrial automation system having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the method comprising:

~~inputting at least one model related to one or more industrial controllers;~~

~~generating one or more security outputs based on the at least one model; and~~

~~automatically installing one or more security components based at least in part on the one or more security outputs;~~

monitoring ~~access to the one or more industrial controllers~~ communication of data associated with the I/O table for a predetermined training period to learn at least one ~~access~~ learned pattern of communication; ~~and~~

defining a pattern threshold specifying an acceptable deviation from the at least one learned pattern;

monitoring data traffic subsequent to the training period; and

performing at least one automated security event if ~~a detected deviation~~ a current pattern of the data traffic deviates from the at least one ~~access~~ learned pattern ~~exceeds a tolerance~~ in excess of the acceptable deviation after the training period[[.]],

wherein performing the at least one automated security event includes at least altering a network traffic pattern between the industrial controller and the I/O device.

13. (Currently Amended) The method of claim 12, ~~wherein inputting the at least one model includes inputting at least one model that is related to at least one of a risk-based model or a cost-based model.~~ further comprising:

inputting at least one model related to one or more industrial controllers;

generating one or more security outputs based on the at least one model; and

automatically installing one or more security components based at least in part on the one or more security outputs.

14. (Currently Amended) The method of claim [[12]] 13, wherein generating the one or more security outputs includes generating one or more security outputs that include at least one of recommended security components, codes, parameters, settings, related interconnection topologies, connection configurations, application procedures, security policies, rules, user procedures, or user practices.

15. (Currently Amended) The method of claim [[12]] 13, further comprising:

automatically deploying the one or more security outputs to the ~~one or more~~ industrial controller[[s]]; and

utilizing the one or more security outputs to mitigate at least one of ~~unwanted~~ unauthorized network access or network attack.

16. (Currently Amended) A security analysis system in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, comprising:

~~means for receiving abstract descriptions of one or more industrial controllers;~~

means for monitoring communication of data associated with the I/O table for a predetermined training period;

means for learning at least one ~~access~~ learned pattern of communication based on the means for monitoring ~~for accessing the one or more industrial controllers~~;

~~means for generating one or more security outputs based on the abstract descriptions;~~

~~means for automatically distributing the one or more security outputs to facilitate network security in the industrial automation environment;~~

means for defining a pattern threshold that specifies an acceptable deviation from the learned pattern;

means for automatically detecting ~~a deviation~~ that a current pattern of communication of the data associated with the I/O table deviates from the ~~at least one access~~ learned pattern ~~that exceeds a threshold~~ in excess of the acceptable deviation after the training period; and

means for performing an automated action that alters [[a]] the current ~~access~~ pattern of communication ~~based at least in part on the detected deviation~~ in response to the detecting.

17. (Currently Amended) A security validation system for use in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the system comprising:

~~a scanner component that automatically interrogates an industrial automation device at periodic intervals for security related data;~~

~~a validation component that automatically assesses security capabilities of the industrial automation device based upon a comparison of the security related data and one or more predetermined security guidelines;~~

~~a security analysis tool that recommends interconnection of one or more industrial automation devices to achieve a specified security goal; and~~

a learning component that monitors communication of data associated with the I/O table with respect to the industrial controller during a training period and establishes a learned pattern of communication; and

an analyzer component that monitors a current pattern of communication of the data associated with the I/O table subsequent to the training period and automatically ~~adjusts at least one security parameter in the industrial automation device~~ performs a security action to bring the current pattern in line with the learned pattern in response to ~~detected security events~~ detecting that the current pattern communication has deviated from the learned pattern of access in excess of a defined pattern threshold.

18. (Cancelled)

19. (Currently Amended) The system of claim 17, ~~the validation component performs at least one of a security audit, a vulnerability scan, a revision check, an improper configuration check, file system check, a registry check, a database permissions check, a user privileges check, a password check, or an account policy check.~~ further comprising:

a scanner component that automatically interrogates at least one of the industrial controller, the I/O device, or the controlled device at periodic intervals for security-related data;

a validation component that automatically assesses security capabilities of the at least one of the industrial controller, the I/O device, or the controlled device based upon a comparison of the security-related data and one or more predetermined security guidelines; and

a security analysis tool that recommends at least one network interconnection to achieve a specified security goal indicated by the predetermined security guidelines.

20. (Currently Amended) The system of claim [[17]] 19, wherein the security guidelines are automatically determined.

21. (Currently Amended) The system of claim 46, wherein the host-based component performs vulnerability scanning and auditing on devices, and the network-based component performs vulnerability scanning and auditing on networks.

22. (Cancelled)

23. (Currently Amended) The system of claim 21, wherein at least one of the host-based component or the network-based component at least one of non-destructively maps a topology of information technology (IT) and industrial automation devices, checks revisions and configurations, checks user attributes, or checks access control lists.

24. (Cancelled)

25. (Currently Amended) The system of claim 17, ~~further comprising a component that initiates a security action in response to the detected security events~~[[,]] wherein the security action includes at least one of automatically correcting the security events, automatically adjusting security parameters, altering network traffic patterns, adding security components, removing security components, ~~firing~~ triggering alarms, automatically notifying entities about detected problems and concerns, generating an error or log file, generating a schema, generating data to re-configure or re-route network connections, updating a database, or updating a remote site.

26-29. (Cancelled)

30. (Currently Amended) An automated security validation system for use in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, comprising:

means for monitoring communication of data associated with the I/O table with respect to the industrial controller during a training period and establishing a learned pattern of communication;

means for defining a pattern threshold specifying an allowable deviation from the learned pattern;

~~means for scanning one or more industrial automation devices for potential security violations;~~

means for monitoring a current pattern of communication of the data associated with the I/O table subsequent to the training period; and

means for initiating a security procedure that ~~adjusts at least one security parameter in the one or more industrial automation devices in response to the potential security violations~~ performs a security action to bring the current pattern in line with the learned pattern if the

means for monitoring identifies that a current access pattern deviates from the at least learned pattern in excess of the allowable deviation[[;]].

~~means for performing at least one of security assessments, security compliance checks, or security vulnerability scanning of the one or more industrial automation devices to mitigate the security violations based at least in part on the initiated security procedure; and~~

~~means for determining whether the automated security validation system conforms to one or more network security standards based on at least one of the security assessments, the security compliance checks, or the security vulnerability scanning.~~

31-40. (Cancelled)

41. (Currently Amended) ~~A security learning system in an automation environment, comprising:~~ The tool of claim 1, further comprising a validation component that periodically monitors the controller following deployment of the one or more security outputs to determine one or more vulnerabilities related thereto.

~~means for scanning a network;~~

~~means for learning access patterns to at least one industrial automation device from the network; and~~

~~means for generating a security event that disables network requests from at least one outside network upon determining that the access patterns are out of tolerance with stored access pattern.~~

42-44. (Cancelled)

45. (Previously Presented) The tool of claim 1, the analyzer component is adapted for partitioned security specification entry and sign-off from various groups.

46. (Currently Amended) The system of claim [[17]] 19, the scanner component and the validation component are at least one of a host-based component or a network-based component.

47. (Previously Presented) The system of claim 21, at least one of the host-based component or the network-based component at least one of determines susceptibility to common network-based attacks, searches for open Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports, scans for vulnerable network services, attempts to gain identity information about end devices that relates to hacker entry, or performs vulnerability scanning and auditing on firewalls, routers, security devices, and factory protocols.

48. (Currently Amended) The system of claim [[1]] 41, the validation component automatically installs one or more security components in response to the one or more vulnerabilities.

49. (Currently Amended) The system of claim 1, wherein the analyzer component further performs an automated action that ~~alters access patterns to the one or more industrial controllers~~ disables network requests from at least one outside network upon detecting ~~a deviation~~ that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation ~~from the at least one of shop floor access patterns, Intranet access patterns, Internet access patterns, or wireless access patterns in excess of a threshold~~.

50. (Currently Amended) The system of claim 12, wherein the at least one automated security event includes at least disabling network attempts to access the ~~one or more~~ industrial controller[[s]].

51. (New) The method of claim 12, wherein the monitoring communication of data comprises at least one of monitoring a number of network requests to or from the industrial controller over a given time frame or monitoring a type of request to or from the industrial controller during the training period.

52. (New) The tool of claim 1, wherein the one or more security outputs alter the data traffic between the controller and the at least one I/O device to restore the learned pattern.